REMARKS

Reconsideration and allowance are respectfully requested.

Regarding the claim objections, claim 30 is canceled. The language "thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data," in claims 1, 15, and 29 is believed properly worded. This is simply like saying "ensuring that operation of the automobile is permitted only under safe conditions." It would be awkward to rephrase "that operation" as "an operation" in this context.

Claim 29 is amended into a format recognized as statutory by the USPTO. It recites:

> computer program encoded in a computer-readable medium executable to configure a processor in a data processing apparatus to manage processor configuration data, the processor, when executing the computer program, being configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain, at least one secure mode being a mode in the secure domain, and a monitor mode, said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode, the processor, when executing said computer program being configured to perform the steps of:

Withdrawal of the rejection under 35 U.S.C. §101 is requested.

All claims stand rejected under 35 U.S.C. §103 for obviousness based on the combination of the teaching of WO 01/46800 (Candelore) and US Patent 5,724,027 (Shipman). This rejection is respectfully traversed.

The claims are concerned with a data processing apparatus that supports both secure and non-secure operation. In secure operation, secure data should not be accessed by a non-secure part of the data processing apparatus. But a security vulnerability may arise when the processor

switches between secure operation (the processor is configured to operate in a secure domain) and non-secure operation (the processor is configured to operate in a non-secure domain). The processor's configuration is determined by processor configuration data held in a storage unit accessible by the processor. When switching from the secure domain to the non-secure domain, the secure processor configuration data must be replaced in the storage unit with the non-secure processor configuration data. Similarly, if the processor is switching from the non-secure domain to the secure domain, this switching requires replacing non-secure processor configuration data in the storage unit with the secure processor configuration data.

This switching is managed by having the processor operate (at least partially) in a monitor mode to execute a monitor program to oversee the switching. Typically, when processor configuration data is changed in the storage unit, it is immediately effective, which may compromise the ability of the monitor program to correctly perform the switch of all of the required processor configuration data (see page 3, lines 16-19 of the specification). In order to overcome this problem, the monitor program uses monitor mode specific processor configuration data when the processor operates in the monitor mode, which ensures that the processor is not affected by the switching of the processor configuration data required to implement the transition from one domain to the other (see page 3, lines 20-25 of the specification).

The Examiner contends that Candelore teaches all but one feature of the independent claims. Applicant respectfully disagrees. Consider first the feature of claim 1 that the data processing apparatus comprises "a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain [and] at least one secure mode being a mode in the secure domain." For this feature the

Examiner points to Figure 1, and the text at page 5, lines 13 to 19 and page 8, lines 7 to 24 of Candelore. This text refers to secure/non-secure modes and secure/non-secure system portions. In Candelore, there is no difference between a "mode" and a "system portion." But in the claims here, a "mode" is different from a "domain." As explained in the specification, the secure and non-secure domains provide a mechanism for handling security at the hardware level. They effectively establish separate worlds: the non-secure world groups all hardware and software accessible to non-secure applications that do not require security, and the secure world groups all hardware and software that is only accessible when executing secure code. In contrast, a mode of operation is only available to certain types of devices such as processors. Figures 3 and 4 provide simple illustrations of the difference between modes and domains, and are described at page 18, line 28 to page 19, line 15 repeated here for convenience:

> Figure 3 illustrates a matrix of processing modes associated with different security domains. In this particular example the processing modes are symmetrical with respect to the security domain and accordingly Mode 1 and Mode 2 exist in both secure and non-secure forms. The monitor mode has the highest level of security access in the system and in this example embodiment is the only mode entitled to switch the system between the non-secure domain and the secure domain in either direction. Thus, all domain switches take place via a switch to the monitor mode and the execution of the monitor program 72 within the monitor mode. Figure 4 schematically illustrates another set of non-secure domain processing modes 1, 2, 3, 4 and secure domain processing modes a, b, c. In contrast to the symmetric arrangement of Figure 3, Figure 4 shows that some of the processing modes may not be present in one or other of the security domains. The monitor mode 86 is again illustrated as straddling the non-secure domain and the secure domain. The monitor mode 86 can be considered a secure processing mode, since the secure status flag may be changed in this mode and monitor program 72 in the monitor mode has the ability to itself set the security status flag it effectively provides the ultimate level of security within the system as a whole.

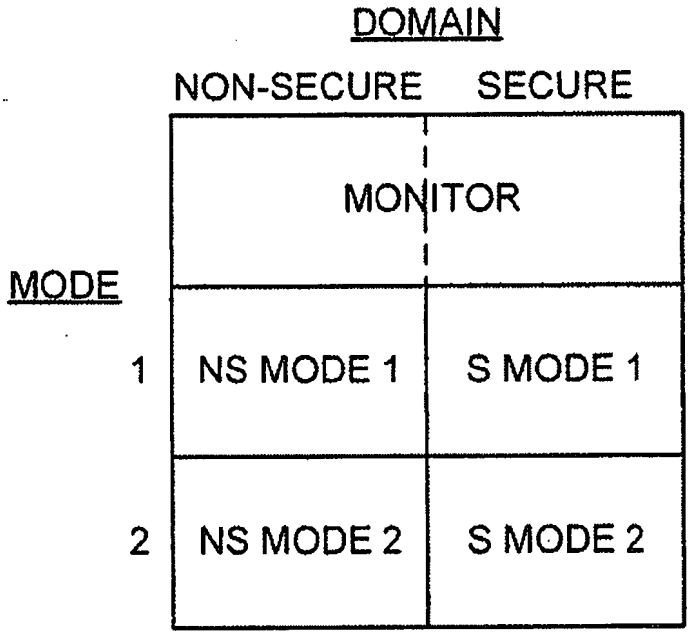
DOMAIN
NON-SECURE
SECURE
MONITOR
MODE
1
NS MODE 1
S MODE 1
2
NS MODE 2
S MODE 2

FIG. 3

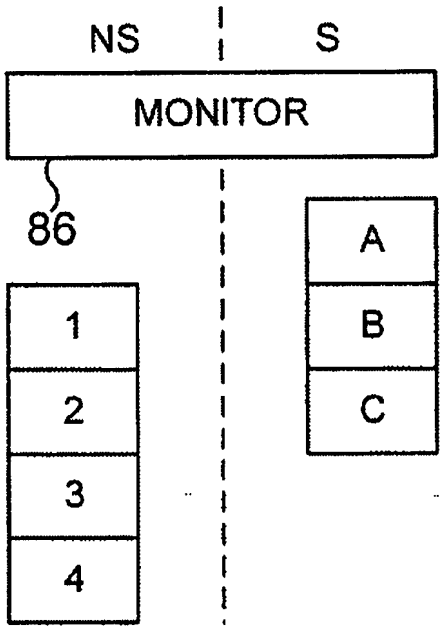
NS
S
MONITOR
86
1
2
3
4
A
B
C

FIG. 4

Next, claim 1 specifies that the plurality of modes includes "a monitor mode." The Examiner points to page 13, lines 26 to 29 of Candelore, which describes a switch device in the context of Figure 4 that issues a mode A/B selection signal (via path 380 in Figure 3). Switching occurs based on time and various time switching patterns as described on page 14. Thus, Candelore describes a system component (a switch) rather that a "mode" in which the processor is configured.

Claim 1 further recites that the data processing apparatus comprises "a storage unit configured to store processor configuration data." Here, the Examiner gives the example from page 16, lines 6 to 11 in Candelore that the most significant bit (MSB) of an address may be used to split the memory between a set of programs A and a set of programs B. As Candelore states at lines 5-6: "This is conceptually similar to switching banks of memory." What Candelore describes is a convenient way to divide address space. The MSB of an address cannot be considered to constitute "processor configuration data." Whether the MSB is set or not determines if the upper memory bank 197 can be used for a set of programs A or the lower memory bank 198 can be used for a set of programs B. As a second contention, the Examiner states that "a mode selection signal is used by the mode A/B timer switcher," referring to the selection signal carried by path 380 in Figure 3 (see page 11, lines 16 to 18). However, this signal simply indicates which mode the processor is currently in, and can not reasonably be considered to be "a storage unit configured to store processor configuration data."

For the claim 1 feature "said switching including switching the processor configuration data in the storage unit between secure processor configuration data and non-secure processor configuration data," the Examiner again points to the MSB function described on page 16, lines 6 to 11 of Candelore. As discussed above, the MSB of the memory address is simply a label to

conveniently divide the memory into two halves. It does not alter "processor configuration data" stored in a storage unit.

The Examiner admits that Candelore does not disclose the processor in the monitor mode executing a monitor program to manage switching between the secure and non-secure domains. The Examiner contends that Shipman teaches this feature pointing to Figure 4 and column 2, lines 10 to 28, and column 4, lines 42 to 46. Figure 4 illustrates keyboard controller states—not operating modes of the processor. Column 2, lines 10 to 28 and the abstract explain that Shipman's teachings specifically relate to the "security" of a keyboard controlling facility, when this security is directed by a system management interrupt (SMI) handler. Furthermore, as in Candelore, Shipman fails to distinguish between a "domain" and a "mode" as the terms are used in the present application.

The last clause of claim 1 specifies that "when in said monitor mode, said monitor program being configured to use monitor mode specific processor configuration data, thereby ensuring that operation of the processor in said monitor mode is unaffected by the switching of the processor configuration data." The Examiner points to Figure 4, column 4, lines 61-63, column 5, lines 52-65, and column 8, lines 64-67 of Shipman. But Shipman fails to disclose "monitor mode specific processor configuration data." The Examiner is requested to identify specifically what data in Shipman and Candelore corresponds to the claimed "monitor mode specific processor configuration data."

Thus, even if these two references could be combined as proposed, they do not teach the combination of features recited in the independent claims, as demonstrated above. Moreover, Shipman relates to an entirely different technical problem: the interaction between a system

management interrupt (SMI) handler and a keyboard controlling facility. How do these teachings from Shipman bring the skilled person closer to what is claimed?

The application is in condition for allowance. An early notice to that effect is earnestly solicited.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____
John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100